CLAIMS

1. A method of controlling access to a network, comprising:

requesting an identity from a client attempting to connect to the network;

receiving the identity;

associating location information with the identity;

authenticating the identity;

comparing the location information against a policy designating locations, if any, at which the client is permitted to connect to the network; and

deciding whether to grant or deny the client access to the network based on the authenticity of the identity and the comparison of the location information.

2. The method of claim 1, further comprising:

passing the identity and the location information to an authentication server, wherein the authentication server performs the steps of authenticating, comparing and deciding.

3. The method of claim 2, wherein the authentication server is a RADIUS server.

4. The method of claim 1, wherein the identity includes information selected from the group consisting of a user name, a user password, a certificate, a media access control (MAC) address, a shared encryption key, a smart card identifier, and any combination of the foregoing information.

5. The method of claim 1, wherein the client is a user station capable of connecting to the network through an access point.

6. The method of claim 1, wherein the client is a wired device capable of connecting to the network through an Ethernet switch port.

7. The method of claim 1, further comprising:

using a mechanism selected from the group consisting of TLS, TTLS, MD5, EAP-TTLS, EAP-TLS, and any combination of the foregoing to authenticate the identity.

8. The method of claim 1, wherein the location information indicates the location of a network switch to which the client is attempting to connect.

9. The method of claim 1, wherein the location information indicates the location of an edge device for connecting the client to the network.

10. A network system, comprising:

an authenticator for requesting an identity from a client and for associating location information with the identity; and

an authentication server, receiving the identity and associated location information from the authenticator, for deciding whether to grant or deny the client access to the network based on the identity and the location information.

11. The network system of claim 10, wherein the authenticator resides in a network switch.

12. The network system of claim 10, wherein the authenticator resides in an edge device.

13. The network system of claim 10, further comprising:

an edge device for connecting a user station to a network switch.

14. The network system of claim 13, wherein the edge device is a wireless access point.

15. The network system of claim 14, wherein the user station is a wireless device capable of connecting to the network through the access point.

16. The network system of claim 10, wherein the client is a wired device capable of connecting to a network switch through an Ethernet port.

17. The network system of claim 10, wherein the location information indicates the location of a network switch to which the client is attempting to connect.

18. The network system of claim 10, wherein the location information indicates the location of an edge device for connecting the client to the network.

19. The network system of claim 18, further comprising an interface for permitting an administrator to associate the location information to the edge device.

20. The network system of claim 10, wherein the authentication server is included in a network switch.

21. The network system of claim 10, wherein the authentication server authenticates the identity.

22. The network system of claim 10, wherein the authentication server includes a policy designating locations, if any, at which the client is permitted to connect to the network.

23. The network system of claim 10, wherein the authentication server is a RADIUS server.

24. The network system of claim 10, wherein the identity includes information selected from the group consisting of a user name, a user password, a certificate, a

media access control (MAC) address, a shared key, a smart card identifier, and any combination of the foregoing information.

25. The network system of claim 10, further comprising a network switch that comprises:

an authentication mechanism selected from the group consisting of TLS, TTLS, MD5, EAP-TTLS, EAP-TLS, and any combination of the foregoing.

26. The network system of claim 10, wherein the authentication server comprises:

an authentication mechanism selected from the group consisting of TLS, TTLS, MD5, EAP-TTLS, EAP-TLS, and any combination of the foregoing.

27. A system, comprising:

a plurality of edge devices capable of communicating with a plurality of user stations over one or more wireless channels;

a network switch including a plurality of ports for connecting the edge devices to a network;

an application running on the network switch, for requesting station identities from the user stations and for associating location information with each of the station identities; and

an authentication server for deciding whether to grant or deny each of the user stations access to the network based on the corresponding identity and location information.

28. The system of claim 27, wherein at least one of the edge devices is a wireless access point.

29. The system of claim 27, further comprising a user station that is a wired device for directly connecting one of the ports of the network switch.

30. The system of claim 27, wherein the location information indicates the location of the network switch.

31. The system of claim 27, wherein the location information indicates the location of one of the edge devices.

32. The system of claim 27, wherein the network switch includes an interface for permitting an administrator to associate the location information to the edge devices.

33. The system of claim 27, wherein the network switch includes an authenticator for authenticating the station identities.

34. The system of claim 27, wherein the authentication server authenticates the station identities.

35. The system of claim 27, wherein the authentication server includes a policy designating locations, if any, at which the user stations are permitted to connect to the network.

36. The system of claim 27, wherein the authentication server is a RADIUS server.

37. The system of claim 27, wherein the station identities includes information selected from the group consisting of a user name, a user password, a certificate, a media access control (MAC) address, a shared key, a smart card identifier, and any combination of the foregoing information.

38. The system of claim 27, further comprising:

an authentication mechanism selected from the group consisting of TLS, TTLS, MD5, EAP-TTLS, EAP-TLS, and any combination of the foregoing.

39. A system for controlling access to a network, comprising:

means for requesting an identity from a client attempting to connect to the network;

means for receiving the identity;

means for associating location information with the identity;

means for authenticating the identity;

means for comparing the location information against a policy designating locations, if any, at which the client is permitted to connect to the network; and

means for deciding whether to grant or deny the user station access to the network based on the authenticity of the identity and the comparison of the location information.

40. The system of claim 39, wherein the identity includes information selected from the group consisting of a user name, a user password, a certificate, a media access control (MAC) address, a shared key, a smart card identifier, and any combination of the foregoing information.

41. The system of claim 39, wherein the client is a wireless device capable of connecting to the network through an access point.

42. The system of claim 39, wherein the client is a wired device capable of connecting to the network through an Ethernet port.

43. The system of claim 39, wherein the authenticating means includes:

an authentication mechanism selected from the group consisting of TLS, TTLS, MD5, EAP-TTLS, EAP-TLS, and any combination of the foregoing.

44. The system of claim 39, wherein the location information indicates the location of a network switch to which the client is attempting to connect.

45. The system of claim 39, wherein the location information indicates the location of a edge device for connecting the client to a network switch.